Amendments to the Claims

This listing of claims will replace all prior version and listings of claims in the application:

Listing of Claims:

1. (Currently amended) A method for determining unauthorized usage of a data communication network, comprising the steps of:

monitoring packet headers of packets exchanged between two hosts on the data communication network;

based on the packet headers, determining the existence of a client/server (C/S) ~~identifying a~~ flow corresponding to a predetermined plurality of packets exchanged between the two hosts that relate to a single service and is characterized by a predetermined C/S flow characteristic;

storing information associating a service that is associated with a determined C/S ~~an identified~~ flow with at least one of the hosts that is associated with the determined C/S ~~identified~~ flow, said service comprising an observed service;

determining if an observed service associated with a particular host is out of profile by comparing the service to a prestored allowed network services profile for the particular host; and

in response to determination that an observed service associated with a particular host is out of profile, providing an output indicating that the observed service is out of profile.

2. (Previously amended) The method of claim 1, further comprising the step of displaying to a user indicia corresponding to the occurrence of particular network services observed in connection with one or more hosts during a monitoring period.

3. (Previously amended) The method of claim 2, further comprising the step of displaying an indication that a predetermined observed network service is in profile and observed during the monitoring period, is in profile and was not observed during the monitoring period, or is not in profile.

4. (Previously amended) The method of claim 1, further comprising the step of:

generating an alarm when an observed network service is not an allowed network service for the particular host.

5. (Previously amended) The method of claim 1, further comprising the step of displaying indicia indicating whether an observed network service is not an allowed network service for a particular host.

6. (Previously amended) The method of claim 1, further comprising the step of building the allowed network services profile based upon network services observed during a profile generation time period.

7. (Previously amended) The method of claim 1, further comprising the step of allowing user editing of the allowed network services profile for particular hosts.

8. (Previously amended) The method of claim 1, further comprising the step of allowing user editing of the allowed network services profile for a block of network addresses corresponding to a plurality of hosts.

9. (Currently amended) A method for determining unauthorized usage of a data communication network, comprising the steps of:

monitoring packet headers of packets exchanged between two hosts on the data communication network;

based on the packet headers, determining the existence of a client/server (C/S) ~~identifying a~~ flow corresponding to a predetermined plurality of packets exchanged

between the two hosts that relate to a single service and is characterized by a predetermined C/S flow characteristic;

storing information associating a service that is associated with a determined C/S ~~an identified~~ flow with at least one of the hosts that is associated with the determined C/S ~~identified~~ flow, said service comprising an observed service;

determining hosts on the network that act as a client and server for each determined C/S ~~identified~~ flow;

determining an allowed network services profile comprising information indicating particular network services that are authorized for use by each one of a plurality of hosts in a predefined group of hosts; and

generating an alarm in response to determination that an observed network service for a particular host in the group of hosts is not included in the allowed network services profile.

10. (Currently amended) A method for determining unauthorized usage of a data communication network, comprising the steps of:

monitoring packet headers of packets exchanged between two hosts on the data communication network;

based on the packet headers, determining the existence of a client/server (C/S) ~~identifying a~~ flow corresponding to a predetermined plurality of packets exchanged between the two hosts that relate to a single service and is characterized by a predetermined C/S flow characteristic;

storing information associating a service that is associated with a determined C/S ~~an identified~~ flow with at least one of the hosts that is associated with the determined C/S ~~identified~~ flow, said service comprising an observed service;

storing an allowed network services port profile for each one of a plurality of hosts in a predefined host group, said profile including information identifying port numbers that are authorized for use by each host in the host group;

determining the port numbers of observed network services used by each host in the predefined host group for each determined C/S ~~identified~~ flow;

comparing the allowed network services port profile with observed network service port numbers; and

generating an alarm when an observed network service port number is not included in the allowed network services port profile.

11. (Previously amended) The method of claim 10, further comprising the step of displaying indicia indicating the observed network service port numbers during a monitoring period.

12. (Previously amended) The method of claim 11, further comprising the step of displaying indications that observed network service port numbers are in profile and observed during the monitoring period, are in profile but not yet observed in the monitoring period, or are not in profile.

13. (Previously amended) The method of claim 12, further comprising the step of displaying indicia indicating that observed network service port numbers are included in the allowed network services port profile.

14. (Previously amended) The method of claim 10, further comprising the step of building the network services port profile based upon network service ports observed during a profile generation time period.

15. (Previously amended) The method of claim 10, further comprising the step of allowing user editing of the allowed network services port profile for the hosts group.

16. (Previously amended) The method of claim 15, further comprising the step of allowing user editing of the allowed network services port profile for a block of network addresses corresponding to the hosts group.

17. (Currently amended) A system for determining unauthorized usage of a data communication network, comprising:

a monitoring device including a processor operative to carry out the steps of:

monitoring packet headers of packets exchanged between two hosts on the data communication network;

based on the packet headers, determining the existence of a client/server C/S ~~identifying a~~ flow corresponding to a predetermined plurality of packets exchanged between the two hosts that relate to a single service and is characterized by a predetermined C/S flow characteristic;

storing information associating a service that is associated with a determined C/S ~~an identified~~ flow with at least one of the hosts that is associated with the determined C/S ~~identified~~ flow, said service comprising an observed service;

determining if an observed service associated with a particular host is out of profile by comparing the service to a prestored allowed network services profile for the particular host; and

in response to determination that an observed service associated with a particular host is out of profile, providing an output indicating that the observed service is out of profile.

18. (Previously amended) The system of claim 17, further comprising a monitor coupled to the monitoring device and operative to display indicia indicating observed network services during a monitoring period.

19. (Previously amended) The system of claim 18, wherein the monitor is further operative to display indicia indicating that an observed network service is not an allowed network service.

20. (Previously amended) The system of claim 17, wherein the process is further operative to build the prestored ~~a~~ network services profile based upon network services observed during a profile generation time period.

21. (Previously amended) The system of claim 17, further comprising an editor coupled to the monitoring device and operative to allow user editing of the allowed network services profile.

22. (Previously amended) The system of claim 21, wherein the editor is further operative to allow user editing of the allowed network services profile for a block of network addresses.

23. (Currently amended) A system for analyzing network communication traffic and determining unauthorized use, comprising:

a processor operative to:

a) monitor the packet headers ~~communication of~~ packets on a data communication network;

b) based on the packet headers, classify the monitored packets into client/server (C/S) flows, wherein a C/S flow corresponds to a predetermined plurality of packets exchanged between two hosts that are associated with a single service on the network;

c) maintain a flow data structure for storing data corresponding to a plurality of C/S flows;

d) maintain a host data structure for storing an allowed network services profile for at least one host; [[and]]

e) analyze the C/S flows in the flow data structure in order to determine if an observed service associated with a particular host is out of profile by comparing the service to the allowed network services profile for the particular host; and

e) in response to determination that an observed service associated with a particular host is out of profile, providing

an output indicating that the observed service is out of profile;

a memory coupled to the processor and operative to store the flow data structure and the host data structure; and

a network interface coupled to the processor operative to receive packets on the data communication network.

24. (Currently amended) The method or system of claims 1, 9, 10, 17, or 23, wherein the predetermined C/S flow characteristic ~~of a flow~~ is selected from the group comprising: the elapse of a predetermined period of time wherein no packets are exchanged between two hosts, the occurrence of a FIN flag, predetermined characteristics of traffic on a given port, the occurrence of a RESET packet, data sent by TCP and acknowledged, UDP packets that are not rejected, and local multicast or broadcast.

25. (Previously presented) The method or system of claims 1, 9, 10, 17, or 23, wherein the step of providing an output or alarm comprises the step of communicating a message to a firewall to drop packets going to or from the particular host.

26. (Previously presented) The method or system of claims 1, 9, 10, 17, or 23, wherein the output or alarm is a notification to a network administrator.

27. (Previously presented) The method or system of claims 1, 9, 10, 17, or 23, wherein the output or alarm is provided to a utilization component selected from the group comprising: network security device, email, SNMP trap message, beeper, cellphone, firewall, network monitor, user interface display to an operator.

28. (Previously presented) The method or system of claims 1, 9, 10, 17, or 23, wherein the single service comprises a port number remaining constant for a plurality of packets.

29. (Previously presented) The method or system of claims 1, 9, 10, 17, or 23, wherein the steps are carried out in a monitoring appliance

30. (Previously presented) The method of claim 29, wherein the monitoring appliance monitors communications among inside hosts and outside hosts.

31. (Previously presented) The method of claim 29, wherein the monitoring appliance is coupled to a network device.

32. (Previously presented) The method of claim 31, wherein the network device is selected from the group comprising: router, switch, hub, tap.

33. (Previously presented) The method of claim 31, wherein the network device is a network security device.

34. (Previously presented) The method or system of claims 1, 9, 10, 17, or 23, wherein the monitoring of packets comprises monitoring packet header information only.

35. (Previously presented) The method or system of claims 1, 9, 10, 17, or 23, wherein the unauthorized use is from an inside address or from an outside address.

36. (Currently amended) The method or system of claims 1, 9, 10, 17, or 23, wherein a service is associated with a determined C/S ~~an identified~~ flow in response to initiation of communications between the two hosts.